全景軟體零信任解決方案

身分鑑別 | 設備鑑別 | 信任推斷

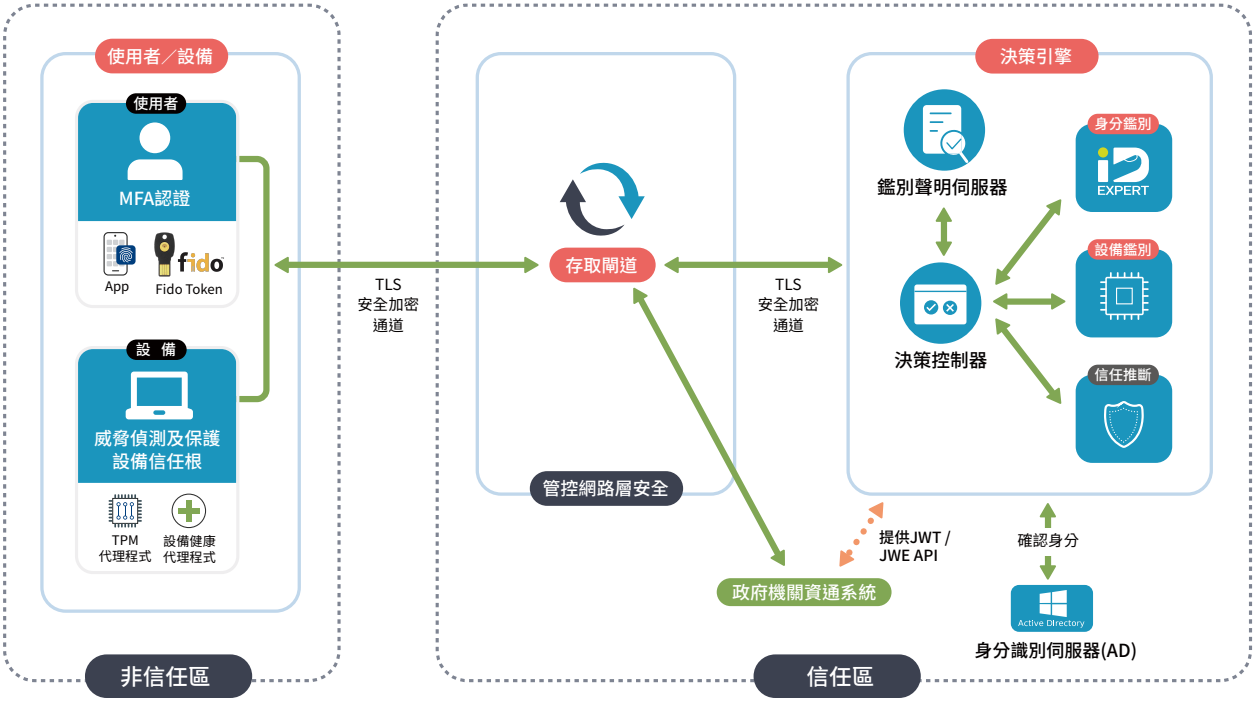
完備零信任架構的驗證需求

CHANG!NG

全景軟體零信任解決方案

APT 攻擊猖獗、遠端存取與行動辦公需求高漲之下，傳統網路安全的邊界防護頻頻遭到突破，全景軟體零信任解決方案將大幅降低企業發生資料外洩風險，以及減少橫向移動攻擊的影響。零信任架構下，如何使用安全 MFA 更是關鍵，全景深耕產業多年，且同時跨足 MFA 及 PKI 領域技術，可滿足政府零信任架構的身分鑑別及設備鑑別階段。

全景軟體零信任架構圖



網路安全：可採取網路原則伺服器 (NPS) 放行，或是使用存取閘道 -Reverse Proxy 方式放行。

鑑別聲明：1 使用 FIDO2 等強認證方式檢查身分 2 檢查設備 TPM 是否有註冊裝置憑證

零信任架構基於「永不信任，持續驗證」的理念，須重複、多方驗證建立信任以讀取資料，其 3 大核心機制：

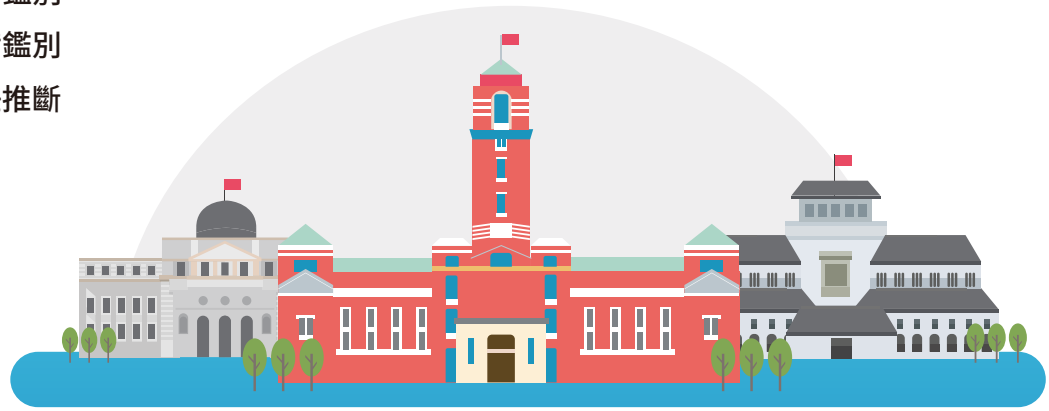
1. 身分鑑別：多因子身分鑑別與身分鑑別聲明。
2. 設備鑑別：設備鑑別與設備健康管理。
3. 信任推斷：使用者情境信任推斷機制。

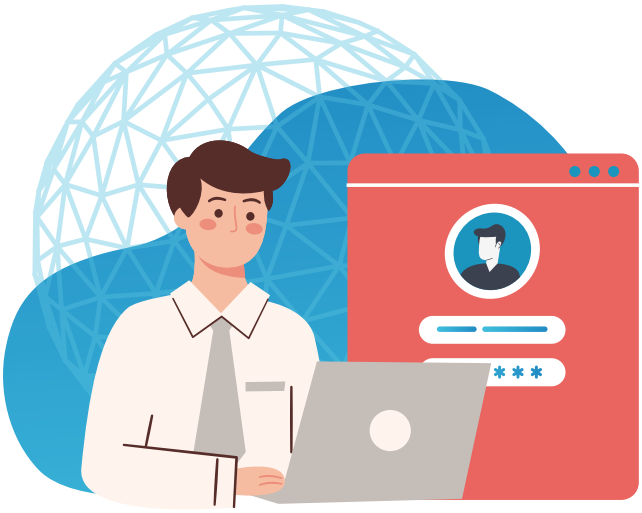
政府推動進程，身分鑑別優先導入

政府推動零信任網路架構，以資通安全責任等級的 A 級公務機關，如總統府、行政院、國安局、國防部、外交部、臺北市等六都市政府等，作為首先導入對象，導入零信任網路架構，並促進國內廠商發展零信任網路資安產業鏈。

111年起遴選機關逐年導入零信任網路

- 111年 身分鑑別
- 112年 設備鑑別
- 113年 信任推斷





保障身分安全，零信任的重要環節

全景身分認證產品通過 FIDO 及 OATH 認證，採用多元的驗證機制，提供多種應用和整合服務，使身分確認的保障可以高效地實施在各產業和政府機關中，進而保障資訊安全，完善網際服務的網路防禦深度和廣度，以主動式防禦機制實現具高強度安全等級的身分認證，守護企業進出門戶。

fido ALLIANCE

oath CERTIFIED

支援一般應用及政府ZTA應用系統

一般應用：

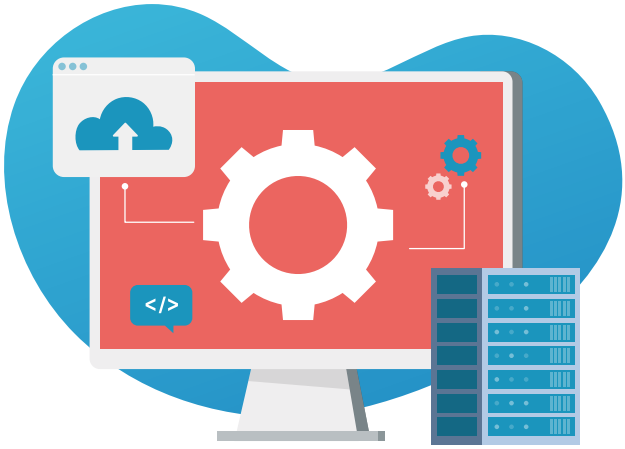
在登入前，須先經過強認證主機後，再進行第二階段登入。

- Windows/ Linux / Mac作業系統
- VPN遠端存取
- VDI遠端辦公連線
- Web網頁服務
- Mail郵件系統

政府ZTA應用系統：

須在身分登入後，取得鑑別聲明，進行驗證及放行。

- 機關資通系統



授權經銷商

CHANGING

全景軟體股份有限公司
www.changingtec.com
TEL : +886-3-563-0688
30844 新竹科學園區新竹縣園區二路48號2樓